

FILED	LODGED
RECEIVED	
FEB 22 2019	
CLERK U.S. DISTRICT COURT WESTERN DISTRICT OF WASHINGTON AT TACOMA BY DEPUTY	

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

15221 105th Ave SE, Yelm, WA 98597 (SUBJECT
PREMISES), and Aaron Anderson (SUBJECT
PERSON)

Case No.

MJ19-5029

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The Subject Premises and Subject Person as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Title 18, U.S.C. § 2252 (a)(2)
 Title 18, U.S.C. § 2252(a)(4)(B)

Offense Description

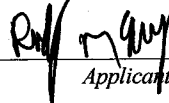
Receipt or Distribution of Child Pornography
 Possession of Child Pornography

The application is based on these facts:

- ☒ See attached Affidavit continued on the attached sheet

- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☐ by reliable electronic means, or: ☐ telephonically recorded.



Applicant's signature

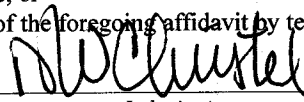
SPECIAL AGENT RICHARD MCKINNEY, FBI

Printed name and title

- ☒ The foregoing affidavit was sworn to before me and signed in my presence, or
☐ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date:

2/22/2019 1005am



Judge's signature

City and state: TACOMA, WASHINGTON

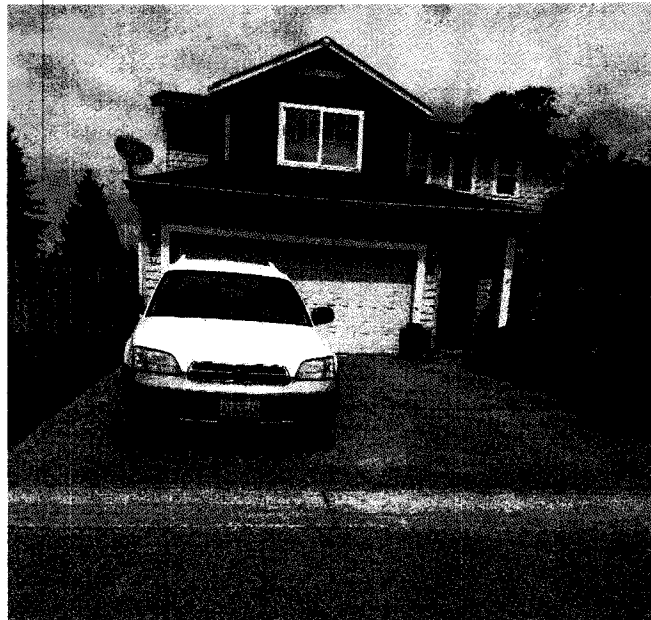
DAVID W. CHRISTEL, United States Magistrate Judge

Printed name and title

ATTACHMENT A

Description of Property to be Searched

The SUBJECT PREMISES is the property located at 15221 105th Ave SE, Yelm, WA 98597, and is more fully described as a two story home with a two car garage in front. The residence was tan with white trim, and had brown shingle-like siding on one street-facing wall above the garage. The garage is located on the West side of the residence and faces south. The front door is located near the center of the residence and faces south.



The search is to include all rooms within the SUBJECT PREMISES, vehicles located on the SUBJECT PREMISES, and all garage/parking spaces or storage units/outbuildings on the SUBJECT PREMISES and any digital device(s) found therein.

1 The SUBJECT PERSON is AARON JAMES ANDERSON (DOB:
2 XX/XX/1982), pictured below:



ATTACHMENT B**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), which may be found at the SUBJECT PREMISES or on the SUBJECT PERSON:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct and child erotica, in any format or media and any items depicted in those visual depictions that may help to identify the person depicted or the creator of the depictions;

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

7. Digital devices and/or their components, which include, but are not limited to:

1 a. Any digital devices and storage device capable of being used to
2 commit, further, or store evidence of the offense listed above;

3 b. Any digital devices used to facilitate the transmission, creation,
4 display, encoding or storage of data, including word processing equipment, modems,
5 docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

6 c. Any magnetic, electronic, or optical storage device capable of
7 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
8 memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives,
9 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

10 d. Any documentation, operating logs and reference manuals regarding
11 the operation of the digital device or software;

12 e. Any applications, utility programs, compilers, interpreters, and other
13 software used to facilitate direct or indirect communication with the computer hardware,
14 storage devices, or data to be searched;

15 f. Any physical keys, encryption devices, dongles and similar physical
16 items that are necessary to gain access to the computer equipment, storage devices or
17 data; and

18 g. Any passwords, password files, test keys, encryption codes or other
19 information necessary to access the computer equipment, storage devices or data;

20 8. Evidence of who used, owned or controlled any seized digital device(s) at
21 the time the things described in this warrant were created, edited, or deleted, such as logs,
22 registry entries, saved user names and passwords, documents, and browsing history;

23 9. Evidence of malware that would allow others to control any seized digital
24 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
25 as evidence of the presence or absence of security software designed to detect malware;
26 as well as evidence of the lack of such malware;

27 10. Evidence of the attachment to the digital device(s) of other storage devices
28 or similar containers for electronic evidence;

1 11. Evidence of counter-forensic programs (and associated data) that are
2 designed to eliminate data from a digital device;

3 12. Evidence of times the digital device(s) was used;

4 13. Any other ESI from the digital device(s) necessary to understand how the
5 digital device was used, the purpose of its use, who used it, and when.

6 14. Records and things evidencing the use of the IP addresses 73.140.63.12 and
7 97.126.88.78 (the SUBJECT IP ADDRESSES) including:

8 a. Routers, modems, and network equipment used to connect
9 computers to the Internet;

10 b. Records of Internet Protocol (IP) addresses used;

11 c. Records of Internet activity, including firewall logs, caches, browser
12 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user
13 entered into any Internet search engine, and records of user-typed web addresses.

14
15 **The seizure of digital devices and/or their components as set forth herein is**
16 **specifically authorized by this search warrant, not only to the extent that such**
17 **digital devices constitute instrumentalities of the criminal activity described above,**
18 **but also for the purpose of the conducting off-site examinations of their contents for**
19 **evidence, instrumentalities, or fruits of the aforementioned crimes.**
20
21
22
23
24
25
26
27
28

AFFIDAVIT

STATE OF WASHINGTON)

) ss

COUNTY OF PIERCE)

I, Richard McKinney, being duly sworn on oath, depose and state:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been employed as an SA since August 2016. I am currently assigned to the Seattle Division of the FBI, Olympia Resident Agency. I completed twenty-and-a-half weeks of training at the FBI academy, including legal classes, investigative techniques, evidence preservation and collection, financial related crimes, and computer related crimes. I am currently authorized to investigate and enforce violations of federal criminal statutes, including those found in Title 18 and 21 of the United States Code. As an SA in the Seattle Division, I have assisted in numerous investigations including but not limited to child pornography, drugs, financial crimes, violent crime, sexual abuse, and child prostitution.

2. I am submitting this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the residence located at 15221 105th Ave SE, Yelm, WA 98597 (hereinafter the "SUBJECT PREMISES") more fully described in Attachment A, and the person of AARON J. ANDERSON (the SUBJECT PERSON), for the things specified in Attachment B to this Affidavit, for the reasons set forth below. I also seek authority to examine digital devices or other electronic storage media. The property and person to be searched is as follows. The warrant would authorize a search of the SUBJECT PREMISES and the SUBJECT PERSON, as well as the seizure and forensic examination of digital devices found therein, for the purpose of identifying electronically stored data as particularly described

1 in Attachment B, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §
2 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. §
3 2252(a)(4)(B) (Possession of Child Pornography).

4 3. The facts set forth in this Affidavit are based on my own personal
5 knowledge; knowledge obtained from other individuals during my participation in this
6 investigation, including other law enforcement officers; review of documents and records
7 related to this investigation; communications with others who have personal knowledge
8 of the events and circumstances described herein; and information gained through my
9 training and experience.

10 4. Because this affidavit is submitted for the limited purpose of establishing
11 probable cause in support of the application for a search warrant, it does not set forth
12 each and every fact that I or others have learned during the course of this investigation. I
13 have set forth only the facts that I believe are relevant to the determination of probable
14 cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §
15 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. §
16 2252(a)(4)(B) (Possession of Child Pornography) will be found at the SUBJECT
17 PREMISES, and on the SUBJECT PERSON.

18 5. Based on the discoveries I have made, as described below, I believe that an
19 individual at the SUBJECT PREMISES has used a computer or other digital media
20 device to connect to and access a foreign website that is well known to law enforcement
21 and commonly used for child exploitation, via Internet Protocol (IP) address
22 73.53.94.225 and distributed at least one image depicting a minor engaged in sexually
23 explicit conduct. I further believe that computers and other digital devices containing
24 evidence of child pornography will be located at the SUBJECT PREMISES and/or on the
25 SUBJECT PERSON.

II. STATEMENT OF PROBABLE CAUSE

A. Background of Investigation

6. On March 20, 2018, the FBI Newark Atlantic City Child Exploitation Task Force (ACCETF) conducted a search warrant at the residence of the subject of two CyberTip reports regarding the uploading of child pornography to a Dropbox account. Agents determined that the subject also distributed child pornography using a Kik messenger account. After examining the subject's smartphone, agents located evidence of multiple Kik group chats in which the subject participated and during with members of the chats posted images and videos of child pornography to the group.

7. Among the users identified in a group chat entitled "Lilly fuck tube" was Kik user "jh7551." On January 26, 2018, jh7551 posted several files to the group. I have reviewed each of these and describe them below:

File 1: This is a color image depicting a prepubescent girl wearing a pink shirt. Her eyes are closed, and her mouth is open. She appears to have male ejaculate on her face. Based on her youthful appearance, stature, and lack of muscular development, I estimate she is between four and six years old.

File 2: This is a color image depicting prepubescent girl lying on her back. Her eyes are partially closed, and she is partially clothed. An adult male hand is holding his penis, which is inserted in the child's mouth. Based on her youthful appearance, stature, and lack of muscular and sexual development, I estimate the child is between six and ten years old.

8. In response to an administrative subpoena, Kik provided the following subscriber information associated with Kik account jh7551:

Name: Jim Henderson
 Email: aaronanderson755@icloud.com (confirmed)
 Username: jh7551
 Registration Timestamp: 09/20/2017 01:10:30 UTC.

1 9. Kik also provided IP connection logs for this account, including data
2 showing that IP address 73.53.94.225 was used to connect to login to Kik account
3 “jh7551” in March 2018. In response to a subpoena for subscriber information associated
4 with this IP address, Comcast Communications reported that this IP address was assigned
5 to the following subscriber and service address throughout March 2018:

6 Subscriber Name: AARON ANDERSON

7 Subscriber Address: 15221 105th Avenue Southeast, Yelm, WA (the SUBJECT
8 PREMISES)

9 Subscriber Email: M_anderson755@comcast.net

10 Subscriber Phone Number: 360-280-1557

11 10. Open source research on username jh7551 revealed a Plenty of Fish (a
12 social media/dating platform) account under the user name “funguy75551.” According to
13 the publicly available “About Me” section of that user’s profile, he is “Just a good
14 looking very normal guy who wants to hang out and get to know and meet new friends. I
15 like outdoor stuff, sports, camping, walking, etc. kik me at jh7551.” This user also has a
16 publicly available profile photo. That photo depicts a person who appears to be the same
17 person pictured in the Washington DOL photo of Aaron Anderson, who lists his address
18 as the SUBJECT PREMISES, 15221 105th Ave SE, Yelm, WA.

19 11. FBI SA Patrick Dospoy conducted surveillance at the residence located at
20 15221 105th Ave SE in Yelm, WA on multiple occasions between May 24, 2018, and
21 September 28, 2018. On May 24, 2018, SA Dospoy observed a white Subaru parked in
22 the driveway with WA license plate ATA2548 with one of the Registered Owners listed
23 as the SUBJECT PERSON.

24 12. On January 8, 2019, SA McKinney conducted surveillance at the residence
25 and observed a maroon Chevrolet Trailblazer parked in the driveway with WA license
26 plate BLY3169. The Trailblazer was registered to M.A., who was listed as a co-owner of
27 the Subaru mentioned above.

28 13. Washington State Department of Licensing records listed two Registered
Drivers, SUBJECT PERSON and M.A., at the SUBJECT PREMISES.

III. PRIOR EFFORTS TO OBTAIN EVIDENCE

14. Any other means of obtaining the necessary evidence to prove the elements of computer/Internet-related crimes, for example, a consent search, could result in an unacceptable risk of the loss/destruction of the evidence sought. If agents pursued a consent-based interview with SUBJECT PERSON, or any other unknown resident(s) or occupant(s) of the SUBJECT PREMISES, they could rightfully refuse to give consent and the user who distributed child pornography files as outlined above could arrange for destruction of all evidence of the crime before agents could return with a search warrant. Based on my knowledge, training and experience, the only effective means of collecting and preserving the required evidence in this case is through a search warrant. Based on my knowledge, no prior search warrant has been obtained to search the SUBJECT PREMISES or the SUBJECT PERSON.

IV. TECHNICAL BACKGROUND

15. Based on my training and experience, when an individual communicates through the Internet, the individual leaves an IP address which identifies the individual user by account and ISP (as described above). When an individual is using the Internet, the individual's IP address is visible to administrators of websites they visit. Further, the individual's IP address is broadcast during most Internet file and information exchanges that occur.

16. Kik is a smartphone messenger application based in Ontario, Canada. Kik lets users communicate through chat. Users can send text, pictures, and videos. Kik is a free messaging and sharing app available on iOS and Android, and uses an existing wireless connection or data plan to communicate with other users. Users can send and receive messages, images, videos, sketches, webpages, memes, gifs, and other content known as bots from within the app. Users can also create groups, which can have up to 50 friends at a time. Users can also create and join public groups with hashtags. Group owners and admins have the capability to add a group name, photos, and remove people from the group. Owners are the group chat originators and Admins are designated by the

1 Owner. As a security feature of Kik, users can be logged into one device per account at a
2 time. When the user tries to log into their account on a second device, Kik will reset on
3 the first device they were signed into, and chat history will then be cleared to protect
4 privacy. When a user creates a Kik account, the following information is collected:

- 5 • First and Last Name
- 6 • Desired Kik Username
- 7 • Email Address
- 8 • Password
- 9 • Birthday
- 10 • Phone Number

11 17. Based on my training and experience, I know that most ISPs provide only
12 one IP address for each residential subscription. I also know that individuals often use
13 multiple digital devices within their home to access the Internet, including desktop and
14 laptop computers, tablets, and mobile phones. A device called a router is used to connect
15 multiple digital devices to the Internet via the public IP address assigned (to the
16 subscriber) by the ISP. A wireless router performs the functions of a router but also
17 includes the functions of a wireless access point, allowing (wireless equipped) digital
18 devices to connect to the Internet via radio waves, not cables. Based on my training and
19 experience, today many residential Internet customers use a wireless router to create a
20 computer network within their homes where users can simultaneously access the Internet
21 (with the same public IP address) with multiple digital devices.

22 18. Based on my training and experience and information provided to me by
23 computer forensic agents, I know that data can quickly and easily be transferred from one
24 digital device to another digital device. Data can be transferred from computers or other
25 digital devices to internal and/or external hard drives, tablets, mobile phones, and other
26 mobile devices via a USB cable or other wired connection. Data can also be transferred
27 between computers and digital devices by copying data to small, portable data storage
28

1 devices including USB (often referred to as "thumb") drives, memory cards (Compact
2 Flash, SD, microSD, etc.) and memory card readers, and optical discs (CDs/DVDs).

3 19. As outlined above, residential Internet users can simultaneously access the
4 Internet in their homes with multiple digital devices. Also explained above is how data
5 can quickly and easily be transferred from one digital device to another through the use
6 of wired connections (hard drives, tablets, mobile phones, etc.) and portable storage
7 devices (USB drives, memory cards, optical discs). Therefore, a user could access the
8 Internet using their assigned public IP address, receive, transfer or download data, and
9 then transfer that data to other digital devices, which may or may not have been
10 connected to the Internet during the date and time of the specified transaction.

11 20. Based on my training and experience, I have learned that the computer's
12 ability to store images and videos in digital form makes the computer itself an ideal
13 repository for child pornography. The size of hard drives used in computers (and other
14 digital devices) has grown tremendously within the last several years. Hard drives with
15 the capacity of four (4) terabytes (TB) are not uncommon. These drives can store
16 thousands of images and videos at very high resolution.

17 21. Based on my training and experience, and information provided to me by
18 other law enforcement officers, I know that people tend to use the same user names
19 across multiple accounts and email services.

20 22. Based on my training and experience, collectors and distributors of child
21 pornography also use online resources to retrieve and store child pornography, including
22 services offered by companies such as Google, Yahoo, Apple, and Dropbox, among
23 others. The online services allow a user to set up an account with a remote computing
24 service that provides email services and/or electronic storage of computer files in any
25 variety of formats. A user can set up an online storage account from any computer with
26 access to the Internet. Evidence of such online storage of child pornography is often
27 found on the user's computer. Even in cases where online storage is used, however,
28 evidence of child pornography can be found on the user's computer in most cases.

1 23. As is the case with most digital technology, communications by way of
2 computer can be saved or stored on the computer used for these purposes. Storing this
3 information can be intentional, i.e., by saving an email as a file on the computer or saving
4 the location of one's favorite websites in, for example, "bookmarked" files. Digital
5 information can also be retained unintentionally, e.g., traces of the path of an electronic
6 communication may be automatically stored in many places (e.g., temporary files or ISP
7 client software, among others). In addition to electronic communications, a computer
8 user's Internet activities generally leave traces or "footprints" and history files of the
9 browser application used. A forensic examiner often can recover evidence suggesting
10 whether a computer contains wireless software, and when certain files under investigation
11 were uploaded or downloaded. Such information is often maintained indefinitely until
12 overwritten by other data.

13 24. Based on my training and experience, I have learned that producers of child
14 pornography can produce image and video digital files from the average digital camera,
15 mobile phone, or tablet. These files can then be easily transferred from the mobile device
16 to a computer or other digital device, using the various methods described above. The
17 digital files can then be stored, manipulated, transferred, or printed directly from a
18 computer or other digital device. Digital files can also be edited in ways similar to those
19 by which a photograph may be altered; they can be lightened, darkened, cropped, or
20 otherwise manipulated. As a result of this technology, it is relatively inexpensive and
21 technically easy to produce, store, and distribute child pornography. In addition, there is
22 an added benefit to the child pornographer in that this method of production is a difficult
23 trail for law enforcement to follow.

24 25. As part of my training and experience, I have become familiar with the
25 structure of the Internet, and I know that connections between computers on the Internet
26 routinely cross state and international borders, even when the computers communicating
27 with each other are in the same state. Individuals and entities use the Internet to gain
28 access to a wide variety of information; to send information to, and receive information

1 from, other individuals; to conduct commercial transactions; and to communicate via
2 email.

3 26. Based on my training and experience, I know that cellular mobile phones
4 (often referred to as "smart phones") have the capability to access the Internet and store
5 information, such as images and videos. As a result, an individual using a smart phone
6 can send, receive, and store files, including child pornography, without accessing a
7 personal computer or laptop. An individual using a smart phone can also easily connect
8 the device to a computer or other digital device, via a USB or similar cable, and transfer
9 data files from one digital device to another. Moreover, many media storage devices,
10 including smartphones and thumb drives, can easily be concealed and carried on an
11 individual's person and smartphones and/or mobile phones are also often carried on an
12 individual's person.

13 27. As set forth herein and in Attachment B to this Affidavit, I seek permission
14 to search for and seize evidence, fruits, and instrumentalities of the above-referenced
15 crimes that might be found at the SUBJECT PREMISES or on the SUBJECT PERSON,
16 in whatever form they are found. It has been my experience that individuals involved in
17 child pornography often prefer to store images of child pornography in electronic form.
18 The ability to store images of child pornography in electronic form makes digital devices,
19 examples of which are enumerated in Attachment B to this Affidavit, an ideal repository
20 for child pornography because the images can be easily sent or received over the Internet.
21 As a result, one form in which these items may be found is as electronic evidence stored
22 on a digital device.

23 28. Based upon my knowledge, experience, and training in child pornography
24 investigations, and the training and experience of other law enforcement officers with
25 whom I have had discussions, I know that there are certain characteristics common to
26 individuals who have a sexualized interest in children and depictions of children:

27 a. They may receive sexual gratification, stimulation, and satisfaction
28 from contact with children; or from fantasies they may have viewing children engaged in

1 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other
2 visual media; or from literature describing such activity.

3 b. They may collect sexually explicit or suggestive materials in a
4 variety of media, including photographs, magazines, motion pictures, videotapes, books,
5 slides, and/or drawings or other visual media. Such individuals often times use these
6 materials for their own sexual arousal and gratification. Further, they may use these
7 materials to lower the inhibitions of children they are attempting to seduce, to arouse the
8 selected child partner, or to demonstrate the desired sexual acts. These individuals may
9 keep records, to include names, contact information, and/or dates of these interactions, of
10 the children they have attempted to seduce, arouse, or with whom they have engaged in
11 the desired sexual acts.

12 c. They often maintain any "hard copies" of child pornographic
13 material that is, their pictures, films, video tapes, magazines, negatives, photographs,
14 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of
15 their home or some other secure location. These individuals typically retain these "hard
16 copies" of child pornographic material for many years, as they are highly valued.

17 d. Likewise, they often maintain their child pornography collections
18 that are in a digital or electronic format in a safe, secure and private environment, such as
19 a computer and surrounding area. These collections are often maintained for several
20 years and are kept close by, often at the individual's residence or some otherwise easily
21 accessible location, to enable the owner to view the collection, which is valued highly.

22 e. They also may correspond with and/or meet others to share
23 information and materials; rarely destroy correspondence from other child pornography
24 distributors/collectors; conceal such correspondence as they do their sexually explicit
25 material; and often maintain lists of names, addresses, and telephone numbers of
26 individuals with whom they have been in contact and who share the same interests in
27 child pornography.

1 f. They generally prefer not to be without their child pornography for
2 any prolonged time period. This behavior has been documented by law enforcement
3 officers involved in the investigation of child pornography throughout the world.

4 g. E-mail itself provides a convenient means by which individuals can
5 access a collection of child pornography from any computer, at any location with Internet
6 access. Such individuals therefore do not need to physically carry their collections with
7 them but rather can access them electronically. Furthermore, these collections can be
8 stored on email "cloud" servers, which allow users to store a large amount of material at
9 no cost, without leaving any physical evidence on the users' computer(s).

10 29. In addition to offenders who collect and store child pornography, law
11 enforcement has encountered offenders who obtain child pornography from the internet,
12 view the contents and subsequently delete the contraband, often after engaging in self-
13 gratification. In light of technological advancements, increasing Internet speeds and
14 worldwide availability of child sexual exploitative material, this phenomenon offers the
15 offender a sense of decreasing risk of being identified and/or apprehended with quantities
16 of contraband. This type of consumer is commonly referred to as a 'seek and delete'
17 offender, knowing that the same or different contraband satisfying their interests remain
18 easily discoverable and accessible online for future viewing and self-gratification. I
19 know that, regardless of whether a person discards or collects child pornography he/she
20 accesses for purposes of viewing and sexual gratification, evidence of such activity is
21 likely to be found on computers and related digital devices, including storage media, used
22 by the person. This evidence may include the files themselves, logs of account access
23 events, contact lists of others engaged in trafficking of child pornography, backup files,
24 and other electronic artifacts that may be forensically recoverable.

25 30. Given the above-stated facts, and based on my knowledge, training and
26 experience, along with my discussions with other law enforcement officers who
27 investigate child exploitation crimes, I believe that the user who possessed and
28 distributed child pornography file(s) to the foreign public photo sharing website likely

1 has a sexualized interest in children and depictions of children and that evidence of child
2 pornography is likely to be found on digital media devices, including mobile and/or
3 portable digital devices that belong to this user or to which this user has access..

4 31. Based on my training and experience, and that of computer forensic agents
5 that I work and collaborate with on a daily basis, I know that every type and kind of
6 information, data, record, sound or image can exist and be present as electronically stored
7 information on any of a variety of computers, computer systems, digital devices, and
8 other electronic storage media. I also know that electronic evidence can be moved easily
9 from one digital device to another. As a result, I believe that electronic evidence may be
10 stored on any digital device present at the SUBJECT PREMISES or on the SUBJECT
11 PERSON.

12 32. Based on my training and experience, and my consultation with computer
13 forensic agents who are familiar with searches of computers, I know that in some cases
14 the items set forth in Attachment B may take the form of files, documents, and other data
15 that is user-generated and found on a digital device. In other cases, these items may take
16 the form of other types of data - including in some cases data generated automatically by
17 the devices themselves.

18 33. Based on my training and experience, and my consultation with computer
19 forensic agents who are familiar with searches of computers, I believe that if digital
20 devices are found in the SUBJECT PREMISES or on the SUBJECT PERSON, there is
21 probable cause to believe that the items set forth in Attachment B will be stored in those
22 digital devices for a number of reasons, including but not limited to the following:

23 a. Once created, electronically stored information (ESI) can be stored
24 for years in very little space and at little or no cost. A great deal of ESI is created, and
25 stored, moreover, even without a conscious act on the part of the device operator. For
26 example, files that have been viewed via the Internet are sometimes automatically
27 downloaded into a temporary Internet directory or "cache," without the knowledge of the
28 device user. The browser often maintains a fixed amount of hard drive space devoted to

1 these files, and the files are only overwritten as they are replaced with more recently
2 viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may
3 include relevant and significant evidence regarding criminal activities, but also, and just
4 as importantly, may include evidence of the identity of the device user, and when and
5 how the device was used. Most often, some affirmative action is necessary to delete ESI.
6 And even when such action has been deliberately taken, ESI can often be recovered,
7 months or even years later, using forensic tools.

8 b. Wholly apart from data created directly (or indirectly) by user-
9 generated files, digital devices - in particular, a computer's internal hard drive - contain
10 electronic evidence of how a digital device has been used, what it has been used for, and
11 who has used it. This evidence can take the form of operating system configurations,
12 artifacts from operating systems or application operations, file system data structures, and
13 virtual memory "swap" or paging files. Computer users typically do not erase or delete
14 this evidence, because special software is typically required for that task. However, it is
15 technically possible for a user to use such specialized software to delete this type of
16 information - and, the use of such special software may itself result in ESI that is relevant
17 to the criminal investigation. In particular, to properly retrieve and analyze electronically
18 stored (computer) data, and to ensure accuracy and completeness of such data and to
19 prevent loss of the data either from accidental or programmed destruction, it is necessary
20 to conduct a forensic examination of the computers. To effect such accuracy and
21 completeness, it may also be necessary to analyze not only data storage devices, but also
22 peripheral devices which may be interdependent, the software to operate them, and
23 related instruction manuals containing directions concerning operation of the computer
24 and software.

25 **V. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES**

26 34. In addition, based on my training and experience and that of computer
27 forensic agents that I work and collaborate with on a daily basis, I know that in most
28 cases it is impossible to successfully conduct a complete, accurate, and reliable search for

1 | electronic evidence stored on a digital device during the physical search of a search site
2 | for a number of reasons, including but not limited to the following:

3 | a. Technical Requirements: Searching digital devices for criminal
4 | evidence is a highly technical process requiring specific expertise and a properly
5 | controlled environment. The vast array of digital hardware and software available
6 | requires even digital experts to specialize in particular systems and applications, so it is
7 | difficult to know before a search which expert is qualified to analyze the particular
8 | system(s) and electronic evidence found at a search site. As a result, it is not always
9 | possible to bring to the search site all of the necessary personnel, technical manuals, and
10 | specialized equipment to conduct a thorough search of every possible digital
11 | device/system present. In addition, electronic evidence search protocols are exacting
12 | scientific procedures designed to protect the integrity of the evidence and to recover even
13 | hidden, erased, compressed, password-protected, or encrypted files. Since ESI is
14 | extremely vulnerable to inadvertent or intentional modification or destruction (both from
15 | external sources and from destructive code embedded in the system such as a "booby
16 | trap"), a controlled environment is often essential to ensure its complete and accurate
17 | analysis.

18 | b. Volume of Evidence: The volume of data stored on many digital
19 | devices is typically so large that it is impossible to search for criminal evidence in a
20 | reasonable period of time during the execution of the physical search of a search site. A
21 | single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A
22 | single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000
23 | double-spaced pages of text. Computer hard drives are now being sold for personal
24 | computers capable of storing up to four terabytes (4,000 gigabytes of data.) Additionally,
25 | this data may be stored in a variety of formats or may be encrypted (several new
26 | commercially available operating systems provide for automatic encryption of data upon
27 | shutdown of the computer).
28 |

1 c. Search Techniques: Searching the ESI for the items described in
2 Attachment B may require a range of data analysis techniques. In some cases, it is
3 possible for agents and analysts to conduct carefully targeted searches that can locate
4 evidence without requiring a time-consuming manual search through unrelated materials
5 that may be commingled with criminal evidence. In other cases, however, such
6 techniques may not yield the evidence described in the warrant, and law enforcement
7 personnel with appropriate expertise may need to conduct more extensive searches, such
8 as scanning areas of the disk not allocated to listed files, or peruse every file briefly to
9 determine whether it falls within the scope of the warrant.

10 35. In this particular case, and in order to protect the third party privacy of
11 innocent individuals residing in the residence, the following are search techniques that
12 will be applied:

13 i. Device use and ownership will be determined through interviews, if
14 possible, and through the identification of user account(s), associated account names, and
15 logons associated with the device. Determination of whether a password is used to lock a
16 user's profile on the device(s) will assist in knowing who had access to the device or
17 whether the password prevented access.

18 ii. Use of hash value library searches.

19 iii. Use of keyword searches, i.e., utilizing key words that are known to be
20 associated with the sharing of child pornography.

21 iv. Identification of non-default programs that are commonly known to be used
22 for the exchange and viewing of child pornography, such as, eMule, uTorrent, BitTorrent,
23 Ares, Shareaza, Gnutella, etc.

24 v. Looking for file names indicative of child pornography, such as, PTHC,
25 PTSC, Lolita, 3yo, etc..

26 vi. Viewing of image files and video files.
27
28

1 vii. As indicated above, the search will be limited to evidence of child
2 pornography and will not include looking for personal documents and files that are
3 unrelated to the crime.

4 36. These search techniques may not all be required or used in a particular
5 order for the identification of digital devices containing items set forth in Attachment B
6 to this Affidavit. However, these search techniques will be used systematically in an
7 effort to protect the privacy of third parties. Use of these tools will allow for the quick
8 identification of items authorized to be seized pursuant to Attachment B to this Affidavit,
9 and will also assist in the early exclusion of digital devices and/or files which do not fall
10 within the scope of items authorized to be seized pursuant to Attachment B to this
11 Affidavit.

12 37. In accordance with the information in this Affidavit, law enforcement
13 personnel will execute the search of digital devices seized pursuant to this warrant as
14 follows:

15 a. Upon securing the search site, the search team will conduct an initial
16 review of any digital devices/systems to determine whether the ESI contained therein can
17 be searched and/or duplicated on site in a reasonable amount of time and without
18 jeopardizing the ability to accurately preserve the data.

19 b. If, based on their training and experience, and the resources
20 available to them at the search site, the search team determines it is not practical to make
21 an on-site search, or to make an on-site copy of the ESI within a reasonable amount of
22 time and without jeopardizing the ability to accurately preserve the data, then the digital
23 devices will be seized and transported to an appropriate law enforcement laboratory for
24 review and to be forensically copied ("imaged"), as appropriate.

25 c. In order to examine the ESI in a forensically sound manner, law
26 enforcement personnel with appropriate expertise will produce a complete forensic
27 image, if possible and appropriate, of any digital device that is found to contain data or
28 items that fall within the scope of Attachment B of this Affidavit. In addition,

1 appropriately trained personnel may search for and attempt to recover deleted, hidden, or
2 encrypted data to determine whether the data fall within the list of items to be seized
3 pursuant to the warrant. In order to search fully for the items identified in the warrant,
4 law enforcement personnel, which may include investigative agents, may then examine
5 all of the data contained in the forensic image/s and/or on the digital devices to view their
6 precise contents and determine whether the data fall within the list of items to be seized
7 pursuant to the warrant.

8 d. The search techniques that will be used will be only those
9 methodologies, techniques and protocols as may reasonably be expected to find, identify,
10 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to
11 this Affidavit.

12 e. If, after conducting its examination, law enforcement personnel
13 determine that any digital device is an instrumentality of the criminal offenses referenced
14 above, the government may retain that device during the pendency of the case as
15 necessary to, among other things, preserve the instrumentality evidence for trial, ensure
16 the chain of custody, and litigate the issue of forfeiture.

17 38. In order to search for ESI that falls within the list of items to be seized
18 pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and
19 search the following items (heretofore and hereinafter referred to as "digital devices"),
20 subject to the procedures set forth above:

21 a. Any digital device capable of being used to commit, further, or store
22 evidence of the offense(s) listed above;

23 b. Any digital device used to facilitate the transmission, creation,
24 display, encoding, or storage of data, including word processing equipment, modems,
25 docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

26 c. Any magnetic, electronic, or optical storage device capable of
27 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
28

1 memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives,
2 camera memory cards, media cards, electronic notebooks, and personal digital assistants;

3 d. Any documentation, operating logs and reference manuals regarding
4 the operation of the digital device, or software;

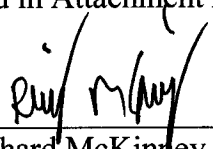
5 e. Any applications, utility programs, compilers, interpreters, and other
6 software used to facilitate direct or indirect communication with the device hardware, or
7 ESI to be searched;

8 f. Any physical keys, encryption devices, dongles and similar physical
9 items that are necessary to gain access to the digital device, or ESI; and

10 g. Any passwords, password files, test keys, encryption codes or other
11 information necessary to access the digital device or ESI.

12 VI. CONCLUSION

13 39. Based on the foregoing, I believe there is probable cause that evidence,
14 fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or
15 Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child
16 Pornography) are located at the SUBJECT PREMISES or on the SUBJECT PERSON as
17 more fully described in Attachment A to this Affidavit, as well as on and in any digital
18 devices found therein. I therefore request that the court issue a warrant authorizing a
19 search of the location, vehicles, and person specified in Attachment A for the items more
20 fully described in Attachment B.

21 
22 Richard McKinley, Affiant
23 Special Agent
24 Federal Bureau of Investigation

25 Subscribed and sworn to before me this 22 day of February, 2019.

26 
27 DAVID W. CHRISTEL
28 United States Magistrate Judge

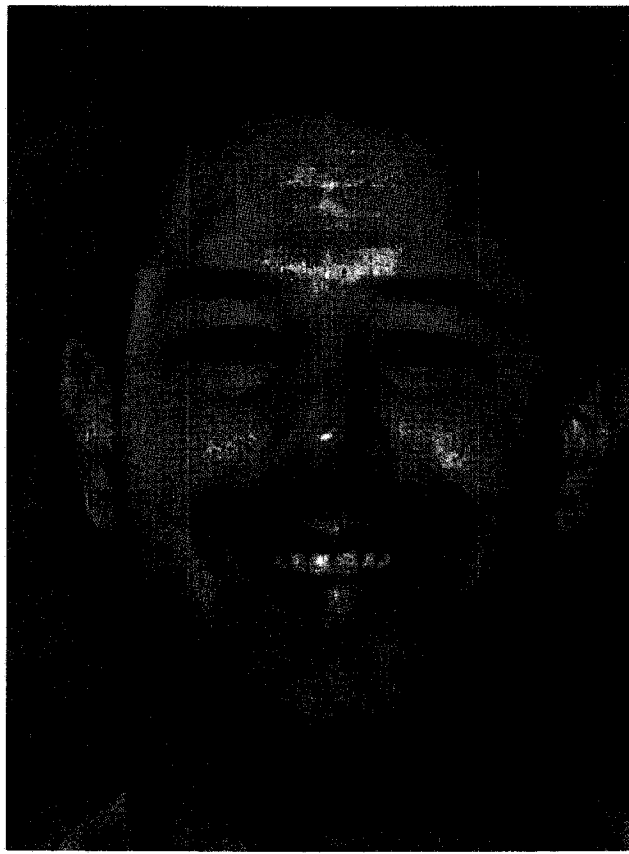
ATTACHMENT A**Description of Property to be Searched**

The SUBJECT PREMISES is the property located at 15221 105th Ave SE, Yelm, WA 98597, and is more fully described as a two story home with a two car garage in front. The residence was tan with white trim, and had brown shingle-like siding on one street-facing wall above the garage. The garage is located on the West side of the residence and faces south. The front door is located near the center of the residence and faces south.



The search is to include all rooms within the SUBJECT PREMISES, vehicles located on the SUBJECT PREMISES, and all garage/parking spaces or storage units/outbuildings on the SUBJECT PREMISES and any digital device(s) found therein.

1 The SUBJECT PERSON is AARON JAMES ANDERSON (DOB:
2 XX/XX/1982), pictured below:



ATTACHMENT B**ITEMS TO BE SEIZED**

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), which may be found at the SUBJECT PREMISES or on the SUBJECT PERSON:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct and child erotica, in any format or media and any items depicted in those visual depictions that may help to identify the person depicted or the creator of the depictions;

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any non-digital recording devices and non-digital media capable of storing images and videos.

7. Digital devices and/or their components, which include, but are not limited to:

- 1 a. Any digital devices and storage device capable of being used to
- 2 commit, further, or store evidence of the offense listed above;
- 3 b. Any digital devices used to facilitate the transmission, creation,
- 4 display, encoding or storage of data, including word processing equipment, modems,
- 5 docking stations, monitors, cameras, printers, encryption devices, and optical scanners;
- 6 c. Any magnetic, electronic, or optical storage device capable of
- 7 storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or
- 8 memory buffers, smart cards, PC cards, memory sticks, flashdrives, USB/thumb drives,
- 9 camera memory cards, media cards, electronic notebooks, and personal digital assistants;
- 10 d. Any documentation, operating logs and reference manuals regarding
- 11 the operation of the digital device or software;
- 12 e. Any applications, utility programs, compilers, interpreters, and other
- 13 software used to facilitate direct or indirect communication with the computer hardware,
- 14 storage devices, or data to be searched;
- 15 f. Any physical keys, encryption devices, dongles and similar physical
- 16 items that are necessary to gain access to the computer equipment, storage devices or
- 17 data; and
- 18 g. Any passwords, password files, test keys, encryption codes or other
- 19 information necessary to access the computer equipment, storage devices or data;
- 20 8. Evidence of who used, owned or controlled any seized digital device(s) at
- 21 the time the things described in this warrant were created, edited, or deleted, such as logs,
- 22 registry entries, saved user names and passwords, documents, and browsing history;
- 23 9. Evidence of malware that would allow others to control any seized digital
- 24 device(s) such as viruses, Trojan horses, and other forms of malicious software, as well
- 25 as evidence of the presence or absence of security software designed to detect malware;
- 26 as well as evidence of the lack of such malware;
- 27 10. Evidence of the attachment to the digital device(s) of other storage devices
- 28 or similar containers for electronic evidence;

1 11. Evidence of counter-forensic programs (and associated data) that are
2 designed to eliminate data from a digital device;

3 12. Evidence of times the digital device(s) was used;

4 13. Any other ESI from the digital device(s) necessary to understand how the
5 digital device was used, the purpose of its use, who used it, and when.

6 14. Records and things evidencing the use of the IP addresses 73.140.63.12 and
7 97.126.88.78 (the SUBJECT IP ADDRESSES) including:

8 a. Routers, modems, and network equipment used to connect
9 computers to the Internet;

10 b. Records of Internet Protocol (IP) addresses used;

11 c. Records of Internet activity, including firewall logs, caches, browser
12 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user
13 entered into any Internet search engine, and records of user-typed web addresses.

14
15 **The seizure of digital devices and/or their components as set forth herein is**
16 **specifically authorized by this search warrant, not only to the extent that such**
17 **digital devices constitute instrumentalities of the criminal activity described above,**
18 **but also for the purpose of the conducting off-site examinations of their contents for**
19 **evidence, instrumentalities, or fruits of the aforementioned crimes.**
20
21
22
23
24
25
26
27
28